

Appl. No. 09/978,200  
Reply to Office Action of: January 12, 2006

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (currently amended) A method of allocating an address to a certificate to enable the storage of said certificate in an addressable database for subsequent retrieval and use in a cryptographic system, said method comprising the steps of:  
~~receiving a certificate request from a correspondent;~~  
~~generating a string for use as a certificate locator, said string being generated from information contained in a request for said certificate, and from information contained in said certificate request;~~  
~~utilizing said string to obtain generate said address for retrieving a corresponding certificate from said database, said certificate being stored at said address; and~~  
~~making said string available for use by said correspondent in generating said address therefrom to retrieve a corresponding certificate from said database.~~
2. (previously presented) A method according to claim 1 wherein said string is mapped to an address in said database.
3. (previously presented) A method according to claim 1 wherein said string is used as said address in said database.
4. (original) A method according to claim 1 wherein a mathematical function is applied to said information to obtain said string.
5. (original) A method according to claim 4 wherein said mathematical function is a hash function.
6. (original) A method according to claim 5 wherein said string is a portion of the output of said hash function.

Appl. No. 09/978,200  
Reply to Office Action of: January 12, 2006

7. (currently amended) A method of identifying to a recipient, an address of a certificate of a signed message in a data communication system, said method comprising the steps of preparing a set of information for inclusion in a certificate request, generating from said set of information a string for use as a certificate locator to enable a corresponding certificate to be located in a database at said address, and forwarding said string to said recipient to enable said recipient to generate said address therefrom, wherein said address indicate indicates the location of said certificate in said database for subsequent retrieval by said recipient.
8. (original) A method according to claim 7 wherein said information includes a time varying element.
9. (original) A method according to claim 7 wherein a predetermined mathematical function is applied to said information to obtain said string.
10. (currently amended) A method for maintaining certificates in a public key infrastructure having a certification authority and a pair of correspondents, said method comprising the steps of collecting at one of said correspondents, information comprising a request for a certificate of said certification authority, forwarding said request to said certification authority, computing a string from said information comprising said request for use as a certificate locator by said one correspondent and said certification authority, generating an address from said string at which said certificate is to be stored, storing [[a]] said certificate issued from said request in a database at [[an]] said address being identifiable from said string, and forwarding said locator string from said one correspondent to another of said correspondents to permit retrieval of said certificate from said database at said address.
11. (original) A method according to claim 10 wherein said information includes a time varying element.
12. (original) A method according to claim 10 wherein communication between said one correspondent and said certification authority is performed over a secure channel.
13. (previously presented) A method according to claim 10 wherein said other correspondent obtains an address of said certificate from a known address of said database and said string.

Appl. No. 09/978,200  
Reply to Office Action of: January 12, 2006

14. (original) A method according to claim 10 wherein said other correspondent forwards said locator to said certification authority for construction of said address.
15. (original) A method according to claim 10 wherein said string is computed by application of a cryptographic hash function at least part of said request.
16. (original) A method according to claim 15 wherein said part includes a time varying element.
17. (previously presented) A method according to claim 15 wherein a portion of the output of said hash function is used as said string.
18. (previously presented) A method according to claim 10 wherein said string is utilised as a pointer to an address in said database.